DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION

(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)

1. CLEARANCE AND SAFEGUARDING

a. FACILITY CLEARANCE REQUIRED: SECRET

b. LEVEL OF SAFEGUARDING REQUIRED: SECRET

2. THIS SPECIFICATION IS FOR: *(X and complete as applicable)*

	a. PRIME CONTRACT NUMBER	
	b. SUBCONTRACT NUMBER	
X	c. SOLICITATION OR OTHER NUMBER: DAAB15-99-R-0006	DUE DATE *(YYMMDD)*: 990802

3. THIS SPECIFICATION IS: *(X and complete as applicable)*

X	a. ORIGINAL *(Complete date in all cases)*		DATE *(YYMMDD)*: 990701
	b. REVISED *(Supersedes all previous specs)*	Revision No.	DATE *(YYMMDD)*
	c. FINAL *(Complete item 5 in all cases)*		DATE *(YYMMDD)*

4. IS THIS A FOLLOW-ON CONTRACT? ☐ YES ☒ NO. If yes, complete the following:

Classified material received or generated under _____ *(Preceding Contract Number)* is transferred to this follow-on contract.

5. IS THIS A FINAL DD FORM 254? ☐ YES ☒ NO. If yes, complete the following:

In response to the contractor's request dated _____, retention of the identified classified material is authorized for the period of _____

6. CONTRACTOR *(Include Commercial and Government Entity (CAGE) Code)*

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*
TBD		

7. SUBCONTRACTOR

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*

8. ACTUAL PERFORMANCE

a. LOCATION	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*
TBD		

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT

Engineering Development and Validation (Architecture) Joint Tactical Radio System (JTRS)

10. THIS CONTRACT WILL REQUIRE ACCESS TO:	YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	X		a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY		X
b. RESTRICTED DATA		X	b. RECEIVE CLASSIFIED DOCUMENTS ONLY		X
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		X	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	X	
d. FORMERLY RESTRICTED DATA		X	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	X	
e. INTELLIGENCE INFORMATION:			e. PERFORM SERVICES ONLY		X
(1) Sensitive Compartmented Information (SCI)		X	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	X	
(2) Non-SCI		X	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	X	
f. SPECIAL ACCESS INFORMATION		X	h. REQUIRE A COMSEC ACCOUNT	X	
g. NATO INFORMATION	X		i. HAVE TEMPEST REQUIREMENTS	X	
h. FOREIGN GOVERNMENT INFORMATION	X		j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	X	
i. LIMITED DISSEMINATION INFORMATION		X	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	X	
j. FOR OFFICIAL USE ONLY INFORMATION	X		l. OTHER *(Specify)*		
k. OTHER *(Specify)*		X			X

12. PUBLIC RELEASE. Any information *(classified or unclassified)* pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release

☐ Direct ☒ Through *(Specify):*

Joint Tactical Radio System 703-588-1056
1700 N Moore St, Ste 1000
Arlington, VA 22209-1901

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.
* In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. *(Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)*

Reference Item 10a: Contractor is authorized to receive Government furnished cryptographic equipment. Access to classified COMSEC information requires a final U.S. Government clearance at the appropriate level. Further disclosure of COMSEC information by a contractor, to include subcontracting, requires prior approval of the contracting activity.

Reference Item 10g: Access up to and including NATO SECRET material will be required for reference only at the Government facility.

Reference 10j: Safeguarding "FOR OFFICIAL USE ONLY" (FOUO) Information - Appendage 2.

Reference Item 11c: All classified information received or generated under this contract is the property of the U.S. Government. At the termination or expiration of this contract, the U.S. Government will be contacted for proper disposition instructions.

Reference Item 11g: The contractor must prepare and process DD Forms 1540 and 1541 through the office listed in block 12 for authorized access to DTIC.

Reference 10a & 11h.: Addiotonal Security Guidlines for COMSEC,- Appendage 1.

Reference 11i: The contractor shall not process classified information by electrical means prior to a DISA TEMPEST evaluation of the equipment/systems and facility, and written DISA certification that the facility meets DISA TEMPEST criteria. In order to expedite the DISA TEMPEST evaluation, the contractor shall provide a list of equipment, to include model number, which is associated with the processing of classified information. In addition, the estimated percentage of classified information processed, cable/conduit runs, a floor plan layout that depicts placement of equipment in relation to other rooms, equipment distances from walls or uncontrolled areas, and physical security being afforded the equipment both during processing and after hours. The above TEMPEST evaluation and DISA approval will not be required if previous DISA approval can be furnished and is no more than 2 years old. The existing approval must be for processing information at the same or higher level and at the same facility and facility ans items of equipment.

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. *(If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.)* ☒ YES ☐ NO

* SEE ATTACHMENT

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. *(If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.)* ☐ YES ☒ NO

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL	b. TITLE	c. TELEPHONE *(Include Area Code)*
MICHAEL C. COX COL, USA	DPM, JTRS-JPO	703-588-1344

d. ADDRESS *(Include Zip Code)*	17. REQUIRED DISTRIBUTION	
Joint Tactical Radio System 703-588-1056 1700 N Moore St, Ste 1000 Arlington, VA 22209-1901	☒	a. CONTRACTOR
	☐	b. SUBCONTRACTOR
	☒	c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
e. SIGNATURE Michael C. Cox	☒	d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
	☒	e. ADMINISTRATIVE CONTRACTING OFFICER
	☒	f. OTHERS AS NECESSARY DISA Industrial Security

DD Form 254 CONTINUATION SHEET:

Item 13 **SECURITY GUIDANCE.**

Reference 11i: Control of compromising Emanations (TEMPEST)- Appendage #3 and Chapter 11, Section 1of the NISPOM.
Classified materiel/information will be protected IAW the NISPOM and NISPOM Supplement, Chapter 5.
Contractor will prepare a OPSEC Plan and submit to the requiring activity for approval.

AR 300-19, Information Systems Security with AMC Supplement.

Item 14 **ADDITIONAL SECURITY REQUIREMENTS.**

Reference Item 10j: DOD Regulation 5400.7, DOD Freedom of Information Act Program. (DOD Regulation 5400.7 is available at http://web7.whs.osd.mil/html/54007r.htm, or by accessing http://www.defenselink.mil/ and clicking on "Publications" then clicking on Freedom of Information Act (FOIA), and finally clicking on Department of Defense (DOD) Freedom of Information Act Program Regulation)

Reference Item 11j: OPSEC requirements apply. The contractor will comply with special OPSEC requirements contained in the contract or addendum thereto.

APPENDAGE # 1 TO DD FORM 254

ADDITIONAL SECURITY GUIDELINES FOR COMSEC

Provided by Security Support Division
Directorate for Intelligence & Information Security

ADDITIONAL COMSEC GUIDELINES

Contractor Generated COMSEC Material: Any material generated by the contractor (including, but not limited to: correspondence, drawings, models, mockups, photographs, schematics, status programs and special inspection reports, engineering notes, computations and training aids) will be classified according to its own content. Classification guidance will be taken from other elements of this Contract Security Classification Specification, DD Form 254, Government furnished equipment or data, or special instructions issued by the Contracting Officer, or his/her duly appointed representative.

REQUIREMENTS

1. Contractor employees or cleared commercial carriers shall not carry classified COMSEC material on commercial passenger aircraft anywhere in the world without the approval of the procuring and/or the administrative contracting officer.

2. No contractor generated COMSEC or government furnished material may be provided to the Defense Technical Information Center (DTIC). Contractor generated technical reports will bear the statement "Not Releasable to the Defense Technical Information Center per DOD Directive 5100-38."

3. No contractor generated COMSEC or government furnished material may be provided to the Defense Documentation Center. Contractor generated technical reports will bear the statement "Not Releasable to the Defense Documentation Center per DOD Instruction 5100.28."

4. Classified paper COMSEC material may be destroyed by burning, pulping, or pulverizing. When a method other than burning is used, all residue must be reduced to pieces 5mm or smaller in any dimension. When classified COMSEC material other than paper is to be destroyed, specific guidance must be obtained from the User Agency.

5. The following downgrading and declassification notation applies to all classified COMSEC information provided to and generated by the contractor:

DERIVED FROM: NSA/CSSM-123-2
DECLASSIFY ON: Source marked "OADR"
DATE OF SOURCE: (Date of document from which information is derived)

6. All contractor personnel to be granted access to classified COMSEC information must be U.S. citizens granted FINAL clearance by the government prior to being given access. Immigrant aliens, interim cleared personnel, or personnel holding a contractor granted CONFIDENTIAL clearance are not eligible for access to classified COMSEC information released or generated under this contract without the express

permission of the Director, NSA. If applicable; contractor personnel having access to TOP SECRET COMSEC material must comply with AR 380-40, Chapter 8 and be registered in the Department of the Army Cryptographic Access Program (DACAP).

7. Unclassified COMSEC information released or generated under this contract shall be restricted in its dissemination to personnel involved in the contract. Release in open literature or exhibition of such information without the express written permission of the Director, NSA, is strictly prohibited.

8. Recipients of COMSEC information under this contract may not release information to subcontractors without permission of the User Agency.

9. The requirements of DOD 5220-22-M National Industrial Security Program Operating Manual (NISPOM) and COMSEC Supplements are applicable to this effort.

10. Additional notices to be affixed to the cover and title or first page of contractor generated COMSEC documents:

a. "COMSEC MATERIAL - ACCESS BY CONTRACTOR PERSONNEL RESTRICTED TO U.S. CITIZENS HOLDING FINAL GOVERNMENT CLEARANCE."

b. "THIS PUBLICATION OR INFORMATION IT CONTAINS MAY NOT BE RELEASED TO FOREIGN NATIONALS WITHOUT PRIOR SPECIFIC APPROVAL FROM THE DIRECTOR, NSA. ALL APPROVALS WILL IDENTIFY THE SPECIFIC INFORMATION AND COPIES OF THIS PUBLICATION AUTHORIZED FOR RELEASE TO SPECIFIC FOREIGN HOLDERS. ALL REQUESTS FOR ADDITIONAL ISSUANCES MUST RECEIVE PRIOR SPECIFIC APPROVAL FROM THE DIRECTOR, NSA."

APPENDAGE# 2 TO DD FORM 254

SAFEGUARDING "FOR OFFICIAL USE ONLY" (FOUO) INFORMATION

Provided by the Security Support Division
Directorate for Intelligence & Information Security

1. The "For Official Use Only" (FOUO) marking is assigned to information at the time of its creation in a DoD User Agency. It is not authorized as a substitute for a security classification marking but it is used on official government information that may be withheld from the public under exemptions 2 through 9 of the Freedom of Information Act.

2. Other non-security markings, such as "Limited Official Use" and "Official Use Only" are used by non-DoD User Agencies for the same type of information and should be safeguarded and handled in accordance with instructions received from such agencies.

3. Use of the above markings does not mean that the information cannot be released to the public, only that it must be reviewed by the Government prior to its release to determine whether a significant and legitimate government purpose is served by withholding the information or portions of it.

4. IDENTIFICATION MARKINGS.

a. An unclassified document containing FOUO information will be marked "FOR OFFICIAL USE ONLY" at the bottom of the front cover (if any), on the first page, on each page containing FOUO information, on the back page, and on the outside of the back cover (if any). No portion marking will be shown.

b. Within a classified document, an individual page that contains FOUO and classified information will be marked at the top and bottom with the highest security classification appearing on the page. If an individual portion contains FOUO information but no classified information, the portion will be marked, "FOUO".

c. Any "FOR OFFICIAL USE ONLY" information released to a contractor by a DoD User Agency is required to be marked with the following statement prior to transfer:

THIS DOCUMENT CONTAINS INFORMATION EXEMPT FROM MANDATORY DISCLOSURE UNDER THE FOIA. EXEMPTIONS _____ APPLY

d. Removal of the "FOR OFFICIAL USE ONLY" marking can only be accomplished by the originator or other competent authority. When "FOR OFFICIAL USE ONLY" status is terminated, all known holders will be notified to the extent practical.

5. DISSEMINATION: Contractors may disseminate "FOR OFFICIAL USE ONLY" information to their employees and subcontractors who have a need for the information in connection with a classified contract.

6. STORAGE: During working hours, "FOR OFFICIAL USE ONLY" information shall be placed in an out-of-sight location if the work area is accessible to persons who do not have a need for the information. During nonworking hours, the information shall be stored to preclude unauthorized access. Filing such material with other unclassified records in unlocked files or desks, is adequate when internal building security is provided during

nonworking hours. When such internal security control is not exercised, locked buildings or rooms will provide adequate after-hours protection or the material can be stored in locked receptacles such as file cabinets, desks or bookcases.

7. **TRANSMISSION**: "FOR OFFICIAL USE ONLY" information may be sent via first-class mail or parcel post. Bulky shipments may be sent by fourth-class mail.

8. **DISPOSITION**: When no longer needed, FOUO information may be disposed of by tearing each copy into pieces to preclude reconstructing, and placing it in a regular trash container or as directed by the User Agency.

9. **UNAUTHORIZED DISCLOSURE**: Unauthorized disclosure of "FOR OFFICIAL USE ONLY" information does not constitute a security violation but the releasing agency should be informed of any unauthorized disclosure. The unauthorized disclosure of FOUO information protected by the Privacy Act may result in criminal sanctions.

APPENDAGE# 3 TO DD FORM 254

CONTROL OF COMPROMISING EMANATIONS (TEMPEST)

Provided by the Security Support Division
Directorate for Intelligence & Information Security

1. Reference: DOD 5220.22-M, National Industrial Security Program Operating Manual.

2. In accordance with guidance referenced above, TEMPEST Countermeasures will only be employed where a threat of exploitation exists. A TEMPEST assessment must be performed by the contractor and be validated by INSCOM TEMPEST elements prior to allocation of Army funds for TEMPEST countermeasures.

3. When electronic equipment is used to process classified information, a written TEMPEST/Risk Analysis will be provided to the contracting officer, or designated representative (Command Tempest Control Officer, AMSEL-MI-CI-A), only if either of the following conditions apply:

a. The contractor will use electronic equipment/ facilities to process TOP SECRET, SCI, SAP, SIOP, Restricted data information; or

b. The contractor does not maintain complete physical access control of the facility, e.g., the contractor is located in a suite.

4. Complete TEMPEST assessments will be protected at a minimum of "FOR OFFICIAL USE ONLY." A classification is warranted if classified threat information on the facility is included or significant vulnerabilities are identified.